Open Directory

Directory Services

Session 610

Open Directory

Directory Services

David M. O’Rourke
Engineering Manager
daveo@apple.com

Overview

- Apple's Open Directory technology
  - What is it
  - What is Directory Services
- Review of Directory Services in Mac OS 10.2
- Future Plans for Panther
- Questions and answers

Open Directory

- Open Directory is a technology name
  - Covers both Client Access Technologies and Server Technologies
  - Adopts and promotes Industry Standard technologies
- Open Directory is built into Mac OS X and Mac OS X Server
  - Been there since 10.0
- Open Sourced as part of Darwin
  - http://developer.apple.com/darwin/projects/opendirectory/

Directory Services History

Server
NetInfo
LDAPv2

Desktop
Server
NetInfo
LDAPv2

NetInfo
LDAPv2,
LDAPv3,
NIS & Flat File,
AppleTalk, SLP,
Rendezvous, SMB

All features of Mac OS 10.2
and more exciting features

Mac OS 10.0

Mac OS 10.1

Mac OS 10.2

Panther

What Is Directory Services?

- Abstraction API for read/write access to system configuration data
  - Users, groups, mount records, and others
  - Authentication abstraction

Directory Services in 10.2

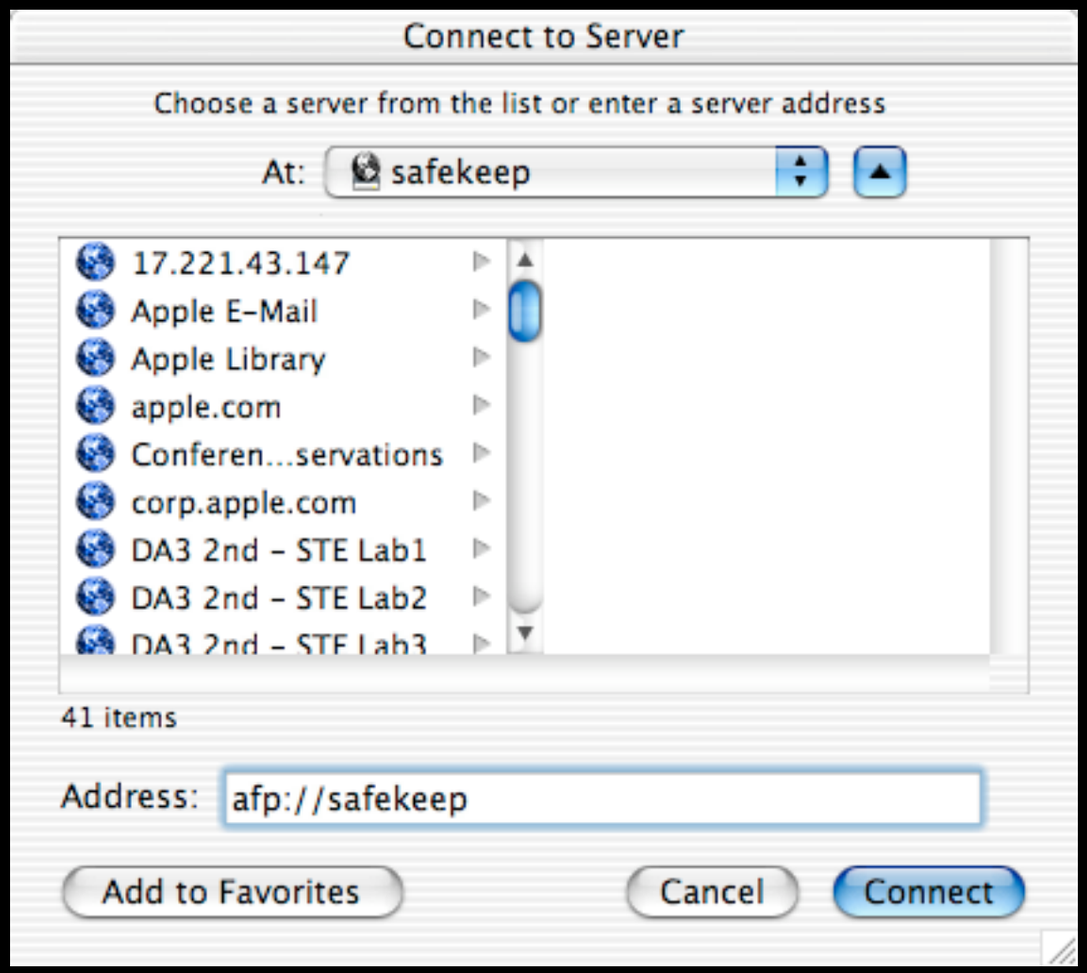
- Includes
  - LDAPv3 (read/write), LDAPv2 (read only), NetInfo, NIS, BSD/etc. files
  - Service Discovery: AppleTalk, SLP, Rendezvous, SMB
- Documented Access API and plug-in API
  - SDK posted
    - Sample code, sample plug-in, notes
  - Directory Services Headers are installed in
    - /System/Library/Frameworks/DirectoryService.framework

10.2 Usage of Directory Services

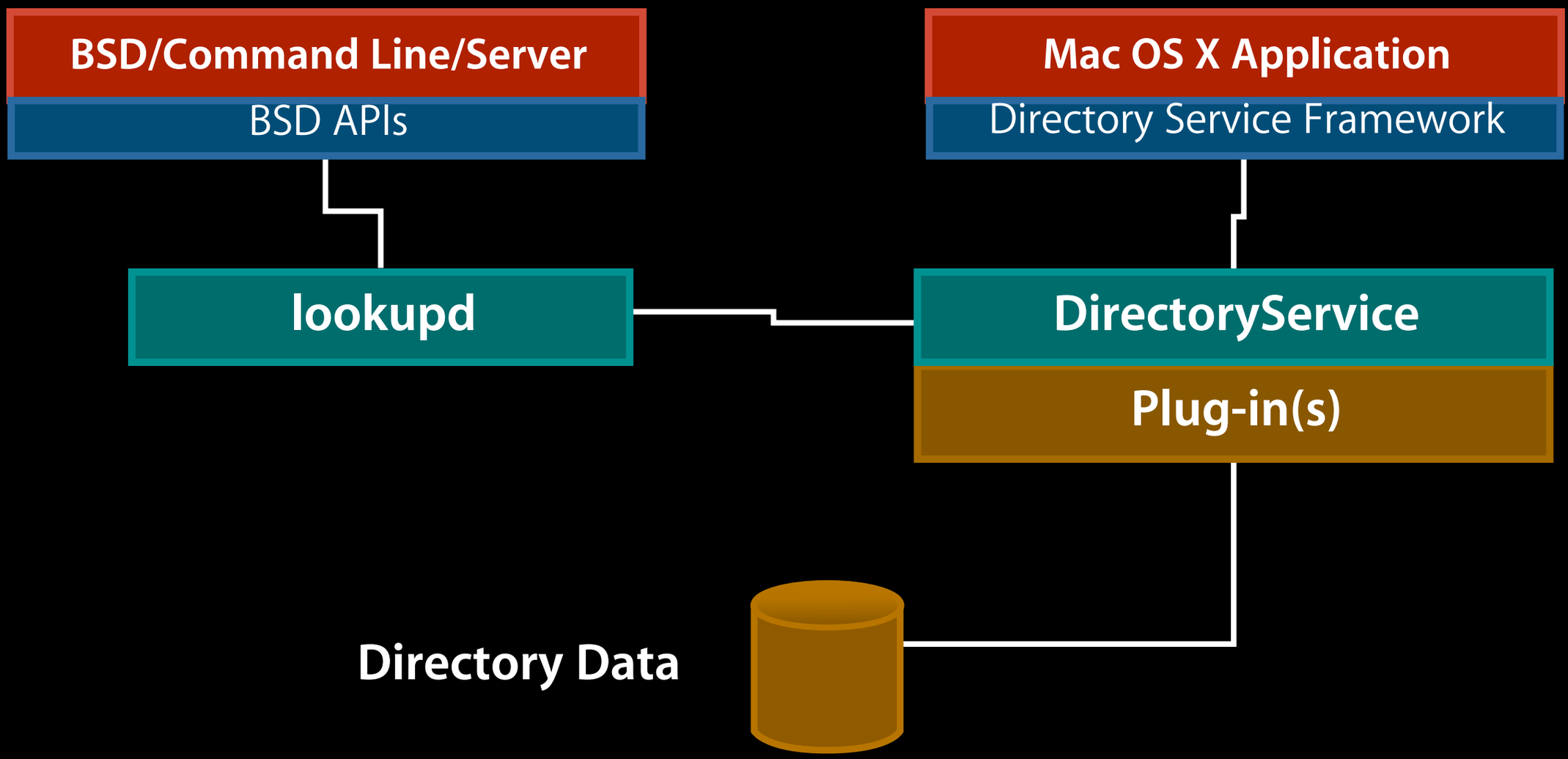
- Login Window uses Directory Services for all user authentication
  - Managed Desktop
- All Security Framework authentication uses Directory Services
- Legacy Unix tools have been migrated to use PAM
  - Mac OS X default PAM module uses Directory Services
- Mac OS X Server processes and Administration Tools

10.2 Connect to Server

- Mac OS 10.2 uses Directory Services for all network browsing
  - Rendezvous, SMB (Windows Networks), SLP, and AppleTalk
  - Use Directory Access to configure which of these network discovery protocols are shown in Connect to Server

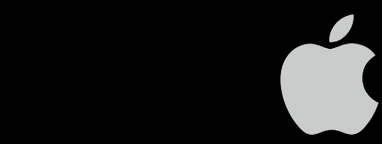


How Does Mac OS 10.2 Use Directory Services?



Mac OS 10.2 Directory Server

- Mac OS 10.2 Server includes two choices for Directory Server
  - NetInfo–Legacy Mac OS X Directory Server
    - Supports Mac OS 10.1 and 10.2
  - LDAPv3–based on OpenLDAP 2.1.x
    - Uses NetInfo database to share data
    - Supports Mac OS 10.2 clients
  - Introduced the Open Directory Password Server
    - SASL-based network authentication



10.2 Review Wrap up

- Jaguar made a lot of progress in the Directory Space
- LDAPv3
- Service Discovery
- New Authentication methods and support

Directory Services for Panther

What's New for Panther

- Enhancements to LDAPv3
- Enhanced Open Directory Password Server support
- Combined NIS/Flat File plug-in
- LDAPv2 is being retired
- Enhanced Support for Active Directory
- Changes to local authentication

What's New for Panther

- Enhanced SMB windows network plug-in
- /Network is now based on NSL/Directory Services
- Directory Services
  - Man pages
  - Command line tool suite
- Minor changes for plug-in developers
  - New standard attributes

LDAPv3 Client Enhancements

- 10.2 LDAPv3 was already a robust LDAPv3 client
  - Support for DHCP LDAP server discovery
  - Server-based or client-side LDAP mappings
  - Integrated support for Open Directory Password Server
- Panther LDAPv3 supports LDAP replication
  - Client side awareness of LDAP replicas
  - API transparent fail over when necessary

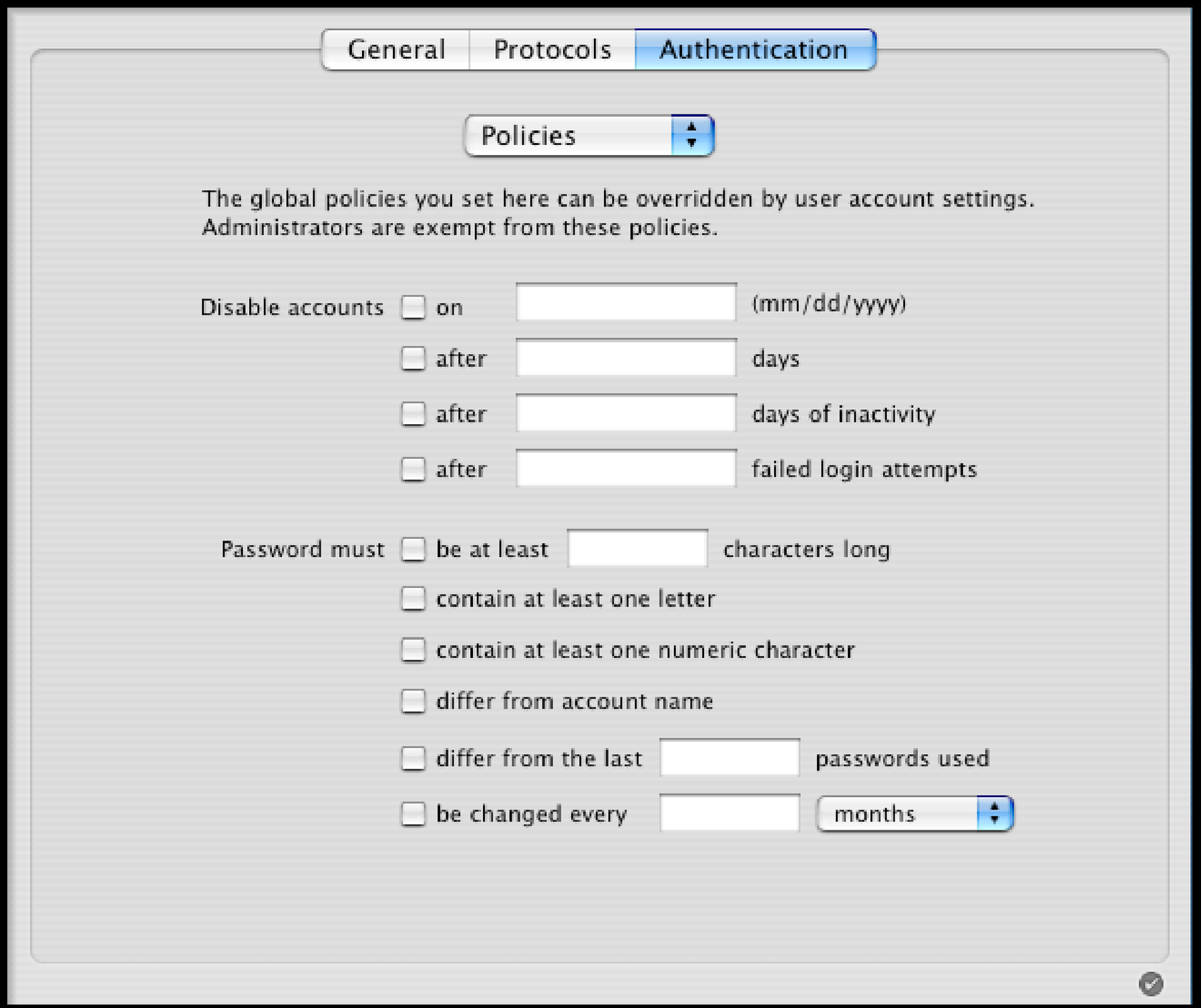
LDAPv3 Client Replica Picking

- LDAPv3 client automatically uses LDAP replicas
- Use any/all of three methods for replica discovery
  - LDAP altServer standard, configuration record, or DNS service records
  - Requires LDAP server connectivity at least once
  - Mac OS X Server LDAP server supports replication
- Replica fail-over resolution is done in parallel

Enhancements to Password Server

- New authentication methods
  - Support for VPN authentication (MS-Chap 2)
  - Support for PDC authentication
- New password policies
  - Global/per-user password policies
- Secure replication
  - True multi-master replication
  - Client side fail over
  - More details in Session #607

Global Policy Screen Shot



Password Server Authentication Methods

Authentication Method	Jaguar	Panther	Protocol Client
MD5 Digest	✓	✓	Default, Login Window, Clear Text
CRAM-MD5	✓	✓	IMAP and SMTP
NT-Lan Manager	✓	✓	SMB File Sharing
APOP	✓	✓	POP3 Mail Protocol
WebDAV Digest	✓	✓	WebDAV File System
MS Chap2		✓	PPP, PPTP, VPN
2 Way Random	✓		AFP
DHX (Diffe-Helman Exhange)	✓	✓	AFP, and Mac OS X Setpassword

Authentication Authority Matrix

Authentication Authority	Example	Comment
;basic;	;basic;	Crypt-based passwords stored in the user record in the password field
;ApplePasswordServer;	;ApplePasswordServer;[ID][PublicKey][Network Address]	Used to indicate password server based user—no readable password hash
;ShadowHash;	;ShadowHash;	Local user account–password hash stored in /var/db/shadow
;Kerberos;	;Kerberos;	Used to indicated a Kerberos based user account

Local Authentication Changes

- Crypt is dead
  - Default local authentication is now stored in a shadow file for all local user accounts
  - Crypt still works–but no tools create crypt users
- Your application should not be relying on crypt passwords
  - Panther will break crypt based applications
  - This is not an OS bug
- Adopt a password verification abstraction

Password Verification Abstractions

- There are 3 major documented abstractions you can use
  - PAM (pluggable authentication modules)
  - Security Framework
  - Directory Services APIs
- If your application is not using one of these APIs, it will break when running on Panther

Password Verification Abstractions

If your application is not using one of these APIs, it will break when running on Panther

Password History and Future

Crypt

Crypt
LDAP Bind
DS API

Crypt
LDAP Bind
Kerberos
DS API
Password Server
PAM
Security Framework

LDAP Bind
Kerberos
DS API
Password Server
PAM
Security Framework

Mac OS 10.0

Mac OS 10.1

Mac OS 10.2

Panther

Authentication Long Term

- Apple is investing heavily in Kerberos
  - Aggressively migrating all networking products to be Kerberos based
  - Apple will ship the MIT KDC
  - Apple already ships the MIT Kerberos client
  - Session #607 and #108 are must attend for any network services
- All Kerberos all the time is in your and Apple's future
- Plan today for the changes you know are coming…

Combined NIS/Flat File Plug-in

- Mac OS 10.2.5 added support for NIS
- Mac OS 10.2 supports/etc configuration files
- Panther's implementation combines the NIS/flat-file support into a single binary/code base
- Unified Configuration HI

NIS/Flat File Configuration Screen

BSD Local configuration

The node /BSD/local must be added to the Authentication and/or Contacts tabs for the configuration information in /etc/ to be used.

NIS Server configuration

Domain Name:

The node /BSD/<domain name> must be added to the Authentication and/or Contacts tabs for NIS to be used.

NIS Servers:

If you don't have a NIS server on your broadcast subnet or want to specify a server for better security, add its name or IP Address to utilize NIS. If you are running on a network with no DNS, you must only use IP address(es).

Cancel OK

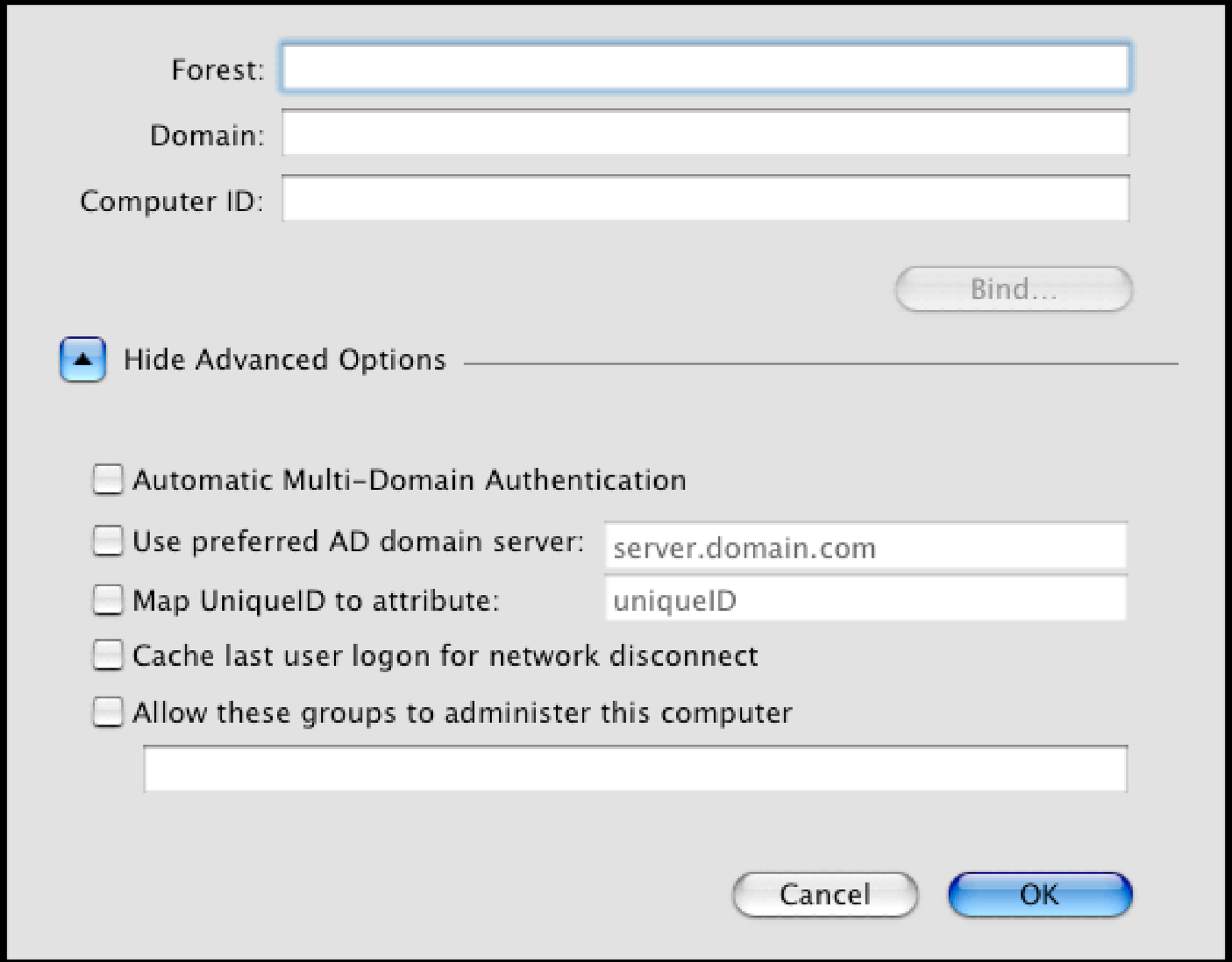
LDAPv2 Is Being Retired

- LDAPv3 plug-in has all LDAPv2 features
  - LDAPv3 is must more robust and has more features
- LDAPv2 configuration automatically converted after first boot
- Apple is working to make this transition seamless
  - Customers should move any existing LDAPv2 deployments to LDAPv3

Active Directory Plug-in

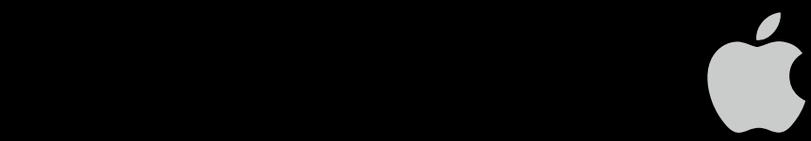
- Apple will provide a native Active Directory plug-in for Open Directory
- Plug-in uses LDAP and Kerberos
- No schema modifications are required
  - Plug-in gererates Mac OS X required attributes
  - Full support for AD features (replication, domain controllers, authentication policies)
- If Mac OS X schema data is present–this plug-in will access that data

Active Directory Configuration



Service Discovery in Panther

- New Windows browsing plug-in
  - Same functionality as Jaguar
  - New feature is the ability to browse Windows networks across subnets
- Rendezvous, AppleTalk, and SLP are still supported
- SLP will be retired in a future OS release
  - Or at least made an optional install
- Move your applications onto Rendezvous



Command Line Tools and Man Pages

- We now have man pages for Directory Services
- We also now have a suite of tools for directory services
  - dscl, pwpolicy, passwd, dsperfmonitor, dserr
- API profiling and kill–USR2
- Server Tools Workgroup manager now includes a new feature called the inspector

Directory Tools Demonstration

Jason Townsend
jtownsend@apple.com

Directory Plug-in Changes

- Lazy plug-in loading
- New standard record and attribute types
- Directory Access plug-ins
- API additions in Panther
- Open Source Update

Lazy Plug-in Loading

- Directory Services will now only load plug-in on first use
- Plug-in authors can support lazy plug-in loading
- Lazy loading improves boot time and memory foot-print for infrequently used Directory systems
- See Apple Developer Relations if you're developing a plug-in
- Changes should only take a couple of hours

Lazy Plug-in Loading

- Two new keys in your plug-in's Info.plist
- DSOKToLoadLazily should be set to "YES"
- DSNodesToRegister is an array of dictionaries specifying nodes to register on your plug-in's behalf

Lazy Plug-in Loading Example

```
<key>DSNodesToRegister</key>
<array>
    <dict>
        <key>DSNodeToRegisterPath</key>
        <array>
            <string>BSD</string>
            <string>local</string>
        </array>
        <key>DSNodeToRegisterType</key>
        <integer>1</integer>
    </dict>
</array>
<key>DSOKToLoadLazily</key>
<string>YES</string>
```

API Additions in Panther

- Umbrella header

```
#include <DirectoryService/DirectoryService.h>
```

- New standard record and attribute types
  - kDSStdRecTypePeople, kDSStdRecTypeAutoServerSetup
  - kDSNAttrKeywords, kDS1AttrXMLPlist
  - See headers for a complete list
- New API for non-user authentication:
  - dsDoDirNodeAuthOnRecordType()

Directory Access Plug-ins

- Directory Access is the configuration tool used to configure Directory plug-ins
  - /Applications/Utilities/Directory Access
- Supported on 10.2 and later
- Provide custom interface for the Configure…button
- Documented in Open Directory Plug-in PDF
- Use Directory Services calls to communicate with your Directory Services plug-in

Directory Access Is a Remote Tool

- Panther Directory Access talking to Jaguar
- Plug-in authors need to provide HI installer for legacy Jaguar plug-ins
  - Work with Apple Developer Relations if your plug-in has HI for configuration

Open Source Update

- Available today
  - DirectoryService (now includes LDAPv3)
  - DSPasswordServerPlugin, passwordserver_sasl
  - DSNSLPlugins, DSAppleTalkPlugin
  - OpenLDAP, netinfo, DSAgent, DSNISPlugin
- Available in Panther timeframe
  - DSTools (includes dscl)
- Obsolete
  - DSFFPlugIn, DSLDAPPlugIn, DSLDAPv3PlugIn

Wrap Up

Summary–Panther changes

- Enhancements to LDAPv3
- Enhanced password Server support
- Combined NIS/Flat File plug-in
- LDAPv2 is being retired
- Enhanced Support for Active Directory
- Changes to local authentication
  - Crypt is dead!
  - Kerberos is coming…

Summary–Panther changes

- Enhanced SMB windows network plug-in
- /Network is now based on NSL/Directory Services
- Directory Services
  - Man pages
  - Command line tool suite
- Minor changes for plug-in developers
  - New standard attributes

Roadmap

101 Security Architectural Overview	The Marina Mon., 5:00pm
108 Kerberos in Mac OS X	The Mission Thur., 9:00am
604 Mac OS X Server Overview	The Mission Tues., 2:00pm
606 Mac OS X Server in Depth	The Marina Tues., 3:30pm
607 Authentication in Mac OS X Server	Nob Hill Tues., 5:00pm
611 Managed Desktop Technologies	Nob Hill Wed., 2:00pm
622 Network Security Best Practices	Nob Hill Fri., 10:30am

Who to Contact

David M. O'Rourke
Engineering Manager
daveo@apple.com

Skip Levens
Server Technology Evangelist
slevens@apple.com

http://developer.apple.com/wwdc2003/urls.html

For More Information

Reference Library

Documentation, Open Source, References

Directory Services API Documentation

http://developer.apple.com/techpubs/macosx/Networking/Open_Directory/index.html

http://developer.apple.com/techpubs/macosx/Networking/Open_Dir_Plugin/index.html

Darwin Open Directory

http://developer.apple.com/darwin/projects/opendirectory/

Open Directory SDK

ftp://ftp.apple.com/developer/Development_Kits/DirectoryServicesSDKv1.0.dmg.bin

Reference Library

Documentation, Open Source, References

Mac OS X Server Documentation

http://www.apple.com/server/macosx/resources.html#g

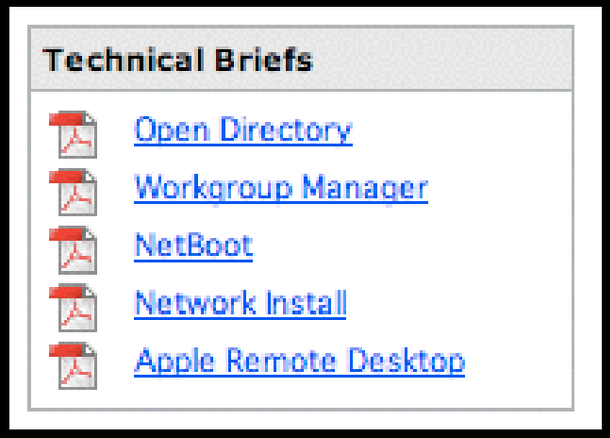
http://www.apple.com/server/desktop_management.html

Mac OS X LDAP schema

Open LDAP Configuration files

Mac OS X Security APIs

http://developer.apple.com/darwin/projects/cdsa/



Reference Library

Documentation, Open Source, References

Open LDAP
http://www.openldap.org/

SASL
http://asg.web.cmu.edu/sasl/

PAM
http://www.kernel.org/pub/linux/libs/pam/

Kerberos
http://web.mit.edu/kerberos/www/

Q&A

David M. O'Rourke
Engineering Manager
daveo@apple.com

http://developer.apple.com/wwdc2003/urls.html

WWDC 2003

Worldwide Developers Conference